Functional Specification for Yukon IED Manager Suite

1. Scope

This specification describes the features and specifications of the Yukon IED Manager Suite (IMS) software.

IMS is an integral part of Eaton's Substation Automation solution. It is designed to work as a standalone product or as a complement to the SMP Gateway family.

IMS is composed of the following modules:

- Enterprise Gateway: Core component that supports communications with field devices, retrieval of non-operational and real-time data.
- Security Server: Provides authentication and authorization services, integration with Active Directory.
- Passthrough Manager: Provides secure remote maintenance access and acts as a NERC CIP compliant Intermediate Device.
- Event Manager: Retrieves fault records and oscillography from protection relays and DFRs.
- Configuration Manager: Retrieves and stores device settings, defines a baseline configuration, monitors for changes, and tracks device configuration change history.
- Password Manager: Manages and updates device passwords.
- Update Manager: Manages firmware updates.

2. Applicable Standards

Product shall be developed under an ISO 9001 certified Quality Management System.

3. Features

3.1. Authentication

3.1.1. The solution shall restrict access to software modules to authenticated users only.

3.1.2. The solution shall support centralized management of user accounts.

3.1.3. The solution shall allow users to be authenticated through their Active Directory accounts.

3.1.4. The solution shall grant access to users according to individual Active Directory accounts.

3.1.5. The solution shall grant access to users according to their membership in Active Directory groups.

3.1.6. The solution shall provide applicative user accounts.

3.1.7. The solution shall allow users to be authenticated through their applicative user accounts.

3.1.8. The solution shall support setting a minimum password length and require password complexity for applicative accounts.

3.1.9. The solution shall support account lockout of applicative accounts after a user-defined number of failed login attempts.

3.1.10. The solution shall support disabling of account lockout of applicative administrative accounts to protect against denial of service.

3.1.11. The solution shall support automatic unlocking of locked-out applicative accounts after a user-defined delay.

3.1.12. The solution shall log all successful and failed login attempts.

3.2. Authorization

3.2.1. The solution shall support Role-Based Access Control.

3.2.2. The solution shall support the capability to assign permissions to groups.

3.2.3. The solution shall organize devices in a hierarchical order of substations and regions.

3.2.4. The solution shall support assigning users to permissions groups.

3.2.5. The solution shall support assigning IEDs, regions and substations to permission groups.

3.2.6. The solution shall support granting permissions to users based on their Active Directory group membership.

3.3. Communications

3.3.1. The solution shall support communications with both serial and networked devices.

3.3.2. The solution shall support low-speed communications links and provide full control of communications settings and timeouts.

3.3.3. The solution shall support devices connected to communications gateways, data concentrators and port switches.

3.3.4. The solution shall support up to four cascaded communications processors or gateways.

3.3.5. The solution shall support SMP Gateway, SEL-2030, and NovaTech Orion gateways.

3.4. Secure Remote Access

3.4.1. The solution shall support NERC CIP compliant remote access to remote devices.

3.4.2. The solution shall implement a layered architecture isolating the client application from the remote IED so that no direct communications between the client application and the remote device is possible.

3.4.3. The solution shall act as a NERC CIP compliant Intermediate Device and provide complete isolation between the client application and the remote device.

3.4.4. The solution shall provide a remote access client application that acts as a port redirector to intercept all communications from a native vendor tool and redirect it to a remote access server.

3.4.5. The solution shall provide a port redirector that supports all protocols commonly used by vendor applications: TELNET, SSH, HTTP, HTTPS, RDP, etc.

3.4.6. The solution shall provide a port redirector that supports vendor applications which simultaneously use multiple TCP/IP ports.

3.4.7. The solution shall provide a port redirector that allows mapping multiple devices to different IP addresses to support vendor tools that allow device selection.

3.4.8. The client application shall support both serial and TCP/IP communications.

3.4.9. The client application shall display a list of available devices from which the user shall select the device to connect.

3.4.10. The client application shall display only the devices to which the user has been granted access.

3.4.11. The client application shall allow the user to select the native vendor tool that will be used to communicate with the device.

3.4.12. The client application shall encrypt all communications between the remote access client and the remote access server (intermediate device) using TLS.

3.4.13. The client application shall be compatible with virtual desktop environments such as Citrix and Microsoft Remote Desktop.

3.4.14. The solution shall perform automatic login to the remote device in order to hide the password to the user, when technically feasible.

3.4.15. The solution shall perform command filtering to prevent users from performing prohibited operations, when technically feasible.

3.4.16. The solution shall support the configuration of access levels and commands that users can perform.

3.4.17. The solution shall log the date and time of the beginning and end of remote access sessions, and identify the computer from which the session was initiated as well as the user login name.

3.4.18. The solution shall automatically terminate the connection to the device after a programmable period of inactivity.

3.4.19. The solution shall record all data exchanged between the client and the end device, to the keystroke level.

3.4.20. The solution shall sanitize the log contents by removing all passwords and IP addresses.

3.4.21. The solution shall provide the capability to disable the logging of critical information such as IP addresses and passwords.

3.4.22. The solution shall provide the capability to enable and disable logging data exchanged with devices.

3.4.23. The solution shall implement optional centralized session management so that remote connections must be enabled by an administrator.

3.4.24. The solution shall provide the capability for a system administrator to view all active connections.

3.4.25. The solution shall provide the capability for a system administrator to terminate a remote connection.

3.5. IED Management

3.5.1. The solution shall implement a web-based user interface application to manage day-to-day operations such as adding devices and accessing reports.

3.5.2. The management application shall support multiple simultaneous users.

3.5.3. The management application shall encrypt all data exchanges using HTTPS.

3.5.4. The management application shall restrict access to authorized users only, on a per device basis.

3.5.5. The management application shall support the grouping of devices by region and substation.

3.5.6. The management application shall support creating, reading, updating and deleting regions, substations and devices.

3.5.7. The management solution shall implement the concept of families of devices that share common characteristics.

3.5.8. The management application shall automatically fill in new device properties from the properties of the selected device family.

3.5.9. The management application shall support the entry of extended device and user-defined properties to be used for asset management and used in reports.

3.5.10. The solution shall log all changes to the system configuration.

3.5.11. The management application shall have the capability to import devices from supported data concentrators.

3.5.12. The management application shall provide a complete set of compliance and operational reports.

3.5.13. The management application shall support customization of existing reports as well as the creation of new user-defined reports.

3.6. Configuration Management

3.6.1. The solution shall provide the capability to connect to supported devices and data concentrators to retrieve configuration settings and firmware version information

3.6.2. The solution shall poll devices and retrieve configuration settings on a scheduled basis, or on demand.

3.6.3. The solution shall store device configuration settings in a centralized database,

3.6.4. The solution shall send out a scan report by email identifying scanned devices and any detected changes in device settings.

3.6.5. The application shall provide the capability to define a set of configuration settings as a device baseline.

3.6.6. The application shall store the name of the user defining the baseline and any notes provides by the user.

3.6.7. The solution shall provide a web-based user interface application to access device configuration settings.

3.6.8. The application shall encrypt all data exchanges using HTTPS.

3.6.9. The application shall restrict access to authorized users.

3.6.10. The application shall provide a summary of devices that are different than their baseline settings.

3.6.11. The application shall display the history of changes detected per device.

3.6.12. The application shall indicate the type of change as being hardware, firmware and settings.

3.6.13. The application shall provide the capability to compare any two sets of configurations settings, from the same device, or from different devices.

3.6.14. The application shall highlight any differences between configurations.

3.6.15. The application shall display the history of changes and baselines for each managed device.

3.6.16. The application shall provide the capability to download stored configuration files and save them to the user's PC.

3.7. Password Management

3.7.1. The solution shall provide the capability to securely store device passwords in a database, view device passwords, request password changes, and print reports.

3.7.2. The solution shall encrypt all passwords stored in the database.

3.7.3. The solution shall support multiple accounts per device.

3.7.4. The solution shall provide the capability to define the password length and complexity requirements by device family, and by individual device type.

3.7.5. The solution shall implement a web-based user interface application to manage device accounts and passwords.

3.7.6. The application shall encrypt all data exchanges using HTTPS.

3.7.7. The application shall restrict access to authorized users only, on a per device basis.

3.7.8. The application shall require different permissions to view passwords and to change passwords.

3.7.9. The application shall display devices organized by region and substation.

3.7.10. The application shall display only the devices to which the user has been granted access.

3.7.11. The application shall display all device accounts.

3.7.12. The application shall display account passwords on demand only.

3.7.13. The application shall hide passwords until display is requested.

3.7.14. The application shall provide the capability to copy a password to the clipboard.

3.7.15. The application shall provide the capability to force the account password in the database.

3.7.16. The application shall provide the capability to force a user-defined password in the database and in the device.

3.7.17. The application shall provide the capability to request a password change for multiple accounts and devices.

3.7.18. The solution shall automatically generate new random passwords according to the length and complexity supported by the device.

3.7.19. The solution shall keep track of all device passwords, the change history, and the previous passwords.

3.7.20. The solution shall support database replication to protect against accidental loss of passwords.

3.7.21. The solution shall change the password in the device as well as any password stored in supported communications gateway or data concentrator.

3.7.22. The solution shall keep track of all passwords that have been exposed and shall print a report on request.

3.7.23. The solution shall keep track of password age and print a report on request.

3.7.24. The solution shall print a report of all current passwords.

3.8. Firmware Updates

3.8.1. The solution shall implement a web-based user interface application to view current device firmware versions and request updates for supported devices.

3.8.2. The application shall restrict access to authorized users only, on a per device basis.

3.8.3. The application shall support different permissions to view firmware version and request firmware update.

3.8.4. The application shall display devices organized by region and substation.

3.8.5. The application shall display only the devices to which the user has been granted access.

3.8.6. The application shall provide the capability to search for devices by name, by firmware version, by model.

3.8.7. The application shall provide the capability to select the firmware version to load on the device.

3.8.8. The application shall provide the capability to request a firmware update immediately, or at a scheduled time.

3.8.9. The application shall provide the capability to request a firmware update for a group of devices.

3.8.10. The application shall provide a dashboard display to track the progress of update operations.

3.8.11. The application shall provide the capability to load the firmware without activating it, for supported devices.

3.8.12. The application shall provide the capability to load a file with updated device settings, for supported devices.

3.8.13. The solution shall print a detailed log of all operations performed, with their success or failure status, during the update process.

3.9. Fault Record Retrieval

3.9.1. The solution shall retrieve fault records from supported devices and data concentrators and store them in a centralized database.

3.9.2. The solution shall provide the capability to copy retrieved event files to a user specified folder for processing by a third party solution.

3.9.3. The solution shall poll devices for the availability of fault records on a scheduled basis, or on demand.

3.9.4. The solution shall provide an API so that a third party application can trigger an event retrieval scan.

3.9.5. The solution shall support the use of a substation data concentrator to retrieve and concentrate event files at the substation level in order to reduce the bandwidth requirement.

3.9.6. The solution shall support the retrieval of fault records using FTP, DNP3 and IEC 61850 file transfer.

3.9.7. The solution shall store retrieved data in the original format so it can be processed by the native vendor tool.

3.9.8. The solution shall advise users by email when fault records are retrieved.

3.9.9. The solution shall send notification email messages containing the data retrieved from the device and a graphic representation of the device targets, when technically feasible.

3.9.10. The solution shall support configuring which events are reported to which user.

3.9.11. The solution shall automatically assign events to user-defined categories.

3.9.12. The solution shall support converting fault records to COMTRADE format.

3.9.13. The solution shall provide a web based user interface application to access retrieved fault records.

3.9.14. The application shall encrypt all data exchanges using HTTPS.

3.9.15. The application shall provide the capability to restrict access to authorized users only.

3.9.16. The application shall display devices organized by region and substation.

3.9.17. The application shall display only devices to which the user has been granted access.

3.9.18. The application shall provide a dashboard displaying the count of events by time period, region and substation.

3.9.19. The application shall provide the capability to display a list of events per device.

3.9.20. The application shall provide the capability to acknowledge events.

3.9.21. The application shall support multiple acknowledgement levels that can be assigned to individual users.

3.9.22. The application shall provide the capability to filter events according to their acknowledgement level and status.

3.9.23. The application shall provide the capability to search for events within a time frame, by region, by substation, by device type, by event type, by acknowledgement status and level.

3.9.24. The application shall support grouping of events, viewing of event groups, and viewing of the events within a group.

3.9.25. The application shall automatically group events occurring within a user selectable time frame.

3.9.26. The application shall provide the capability to download events in native or COMTRADE format.

3.9.27. The application shall provide the capability to download a group of events as a ZIP file.

3.10. Common Requirements

3.10.1. The solution shall support multiple simultaneous users.

3.10.2. The solution shall implement a multi-threaded approach to support operations simultaneously on multiple devices.

3.10.3. The solution shall provide secure web interfaces for common operations and will not require the installation of a client application on the user's PC.

3.10.4. All user interface applications shall display an appropriate use banner.

3.10.5. Web-based applications shall encrypt all data exchanges using HTTPS.

4. Licensing

4.1. The licensing model shall be flexible and scalable.

4.2. The solution shall support licensing modules individually.

4.3. The solution shall support licensing modules based on the number of managed IEDs per module.

5. Operating System

5.1. The application shall support the following operating systems:

- Windows Server 2008 R2
- Windows Server 2012 R2

5.2. The application shall support the following databases:

- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

5.3. The solution shall be compatible with Microsoft server redundancy options.

5.4. The solution should publish all logs using Syslog.

6. Virtualization

6.1. The solution shall support common virtualization solutions:

- Microsoft Hyper-V
- VMware ESX and VMware ESXi
- Citrix XenApp